Pravidla pro připojení do projektu FENIX

1. ÚVODNÍ USTANOVENÍ

1.1. Tato Pravidla upravují podmínky připojení do projektu FENIX zřízeného shora uvedenými zakladateli v rámci NIX.CZ, z.s.p.o. (dále jen „**FENIX** “).

1.2. FENIX se zřizuje v souladu s Platným provozním řádem a ceníkem služeb a stanovami NIX.CZ, z.s.p.o. (dále jen „**NIX.CZ**“).

1.3. Tato Pravidla se v plném rozsahu vztahují i na Zakladatele, a to včetně případného vyloučení z projektu FENIX.

1.4. FENIX je založen jako projekt v oblasti kybernetické bezpečnosti a slouží zejména jako nouzový prostředek vzájemné komunikace členů a zákazníků sdružení NIX.CZ s vysokým prvkem důvěry a zabezpečení pro případ masivních útoků na internetovou infrastrukturu.

1.5. Smyslem vzniku projektu FENIX je umožnit spojení poslední šance („last resort“) v případě, že se infrastruktura člena projektu FENIX stane cílem útoku.

1.6. Připojení do projektu FENIX je bezplatné.

1.7. NIX.CZ není Zakladatelem, je však součástí projektu FENIX, může do něj být kdykoliv připojen a je oprávněn jej užívat stejně jako členové projektu FENIX.

2. PODMÍNKY ZAŘAZENÍ NOVÝCH ČLENŮ ČI ZÁKAZNÍKŮ NIX.CZ DO PROJEKTU FENIX

2.1. Členem projektu FENIX se může stát jen člen nebo zákazník, který je připojen do jakéhokoliv uzlu NIX.CZ déle než 6 měsíců.

2.2. V písemné žádosti o členství v projektu FENIX musí žadatel doložit:

2.2.1. doporučení k přijetí nejméně dvou stávajících členů projektu FENIX na úrovni zodpovědných rolí uvedených v kontaktní databázi NIX.CZ, přičemž tito stávající členové nejsou s žadatelem součástí jednoho podnikatelského seskupení (jsou vzájemně ekonomicky nezávislí),

2.2.2. čestné prohlášení k doložení splnění podmínek dle článku 2 (vyjma bodu 2.5.9),

2.2.3. popis způsobu realizace podmínky uvedené v bodu 2.5.9,

2.2.4. závazek dodržování Pravidel,

2.2.5. kopie svých vzorových smluv či smluvních podmínek se zákazníky.

2.3. K žádosti o členství v projektu FENIX se může vyjádřit kterýkoliv stávající člen projektu FENIX. V případě, že ve lhůtě 14 dnů ode dne informování stávajících členů projektu FENIX o žádosti o členství nebude nejméně jednou šestinou stávajících členů vznesen protest, může být žadatel do projektu FENIX připojen a stát se jejím členem. Na přijetí do projektu FENIX není dán právní nárok ani v případě, že jsou splněny všechny podmínky dle článku 2.5.

2.4. Členem projektu FENIX se nemůže stát zákazník NIX.CZ, který je v rámci partnerského programu připojen do uzlu NIX.CZ prostřednictvím jiného člena či zákazníka NIX.CZ jako partnera.

2.5. Platnou žádost o připojení do projektu FENIX může podat člen nebo zákazník NIX.CZ, který

2.5.1. se aktivně účastní pracovních skupin a je-li členem, pak i hlasování v orgánech NIX.CZ, a to alespoň jednou ročně;

2.5.2. nemá vůči NIX.CZ žádné závazky po lhůtě splatnosti a v posledních 6 měsících neměl vůči NIX.CZ žádné závazky po lhůtě splatnosti po dobu delší než 14 dnů;

2.5.3. se nedopouští, a v minulosti se nedopustil, opakovaného ani podstatného porušení provozního řádu NIX.CZ či stanov NIX.CZ;

2.5.4. provozuje plně redundantní, a na sobě nezávislé přípojky do nejméně dvou uzlů NIX.CZ tak, aby v případě výpadku všech přípojek do jednoho uzlu NIX.CZ byly ostatní schopny automaticky převzít a přenést bez přetížení veškerý datový provoz vyměňovaný s partnery v NIX.CZ. Přetížením se rozumí překročení hranice 95. percentilu souhrnného provozu na ostatních přípojkách; ([1])

2.5.5. smluvně zakazuje svým zákazníkům zneužívání sítě (spamming, útoky apod.);

2.5.6. provozuje ve své síti zároveň protokol IPv4 i IPv6 a přiděluje je svým zákazníkům, přičemž oba protokoly aktivně používá k propojení do uzlů NIX.CZ. Prostřednictvím protokolu IPv4 a IPv6 zpřístupňuje svým zákazníkům své služby (např. webové prezentace a DNS servery);

2.5.7. má své domény, pod kterými komunikuje se svými zákazníky či obchodními partnery (včetně webů společnosti a produktových webů), podepsané pomocí technologie DNSSEC, tak aby použité algoritmy odpovídaly aktuálním bezpečnostním standardům, s výjimkou situací, kdy nasazení podepisování brání vážné technické důvody, a má zapnutou DNSSEC validaci na provozovaných resolverech;

2.5.8. má dohledové středisko (NOC) bezproblémově fungující v režimu 24x7 s alespoň jedním telefonickým kontaktem bez obtíží dosažitelným i v případě masivního DDoS útoku na internetovou infrastrukturu člena zveřejněným v intranetu NIX.CZ, přičemž telefonické spojení je směřováno přímo na techniky schopné řešit problém a nesmí být realizováno přes IVR;

2.5.9. ve své síti nebo její části, kterou oznamuje do FENIX VLAN, používá filtrování zdrojových adres (zabránění IP spoofingu) ve smyslu BCP-38 či SAC004. Pro IP adresy v rámci vlastních AS musí být granularita alespoň /24 u IPv4 a /48 u IPv6 s výjimkou prefixů oznamovaných pro speciální účely (jako např. RTBH, DDoS Protector, FlowSpec pravidla apod.). Prefixy sítí získané v rámci FENIX VLAN smí být oznamované pouze těm AS, jejichž prefixy jsou dostupné v rámci FENIX VLAN;

2.5.10. má systém na detekci a likvidaci zdrojů útoku typ amplification (například DNS, SNMP, NTP, zákaz nespravovaných otevřených resolverů, implementace response rate limiting);

2.5.11. monitoruje páteřní linky i zákaznické přípojky alespoň z hlediska toků a přenášených paketů (například MRTG či obdobné), monitoring musí umět aktivně upozornit na vybočení sledovaných hodnot z běžného intervalu;

2.5.12. nepropaguje pomocí BGP protokolu jiné rozsahy, než ke kterým je oprávněn;

[1] V plovoucím časovém období posledních 720 hodin musí být ostatní přípojky schopné absorbovat veškerý datový provoz vyměňovaný s partnery v NIX.CZ s tolerancí/s výjimkou libovolných 432 pětiminutových intervalů (reprezentují 5 procent ze 720 hodin) v rámci tohoto období, ve kterých dosáhl tento provoz nejvyššího objemu (jde tedy o 432)
provozně nejvýznamnějších pětiminutových intervalů, které se při vyhodnocení ignorují).

2.5.13. neposílá ze své sítě do FENIX VLAN provoz z rozsahů, které není oprávněn ze své sítě propagovat;

2.5.14. své routery chrání v souladu s doporučením RFC 6192 (control plane policy) nebo jiným srovnatelně účinným způsobem;

2.5.15. provozuje CERT/CSIRT tým, alespoň se statusem „listed“ u úřadu Trusted Introducer (http://www.trusted-introducer.org);

2.5.16. má zavedeny vnitřní procesy pro řešení incidentů;

2.5.17. zahájí práce na odstranění/omezení bezpečnostního incidentu co nejrychleji, nejpozději do 30 minut od jeho nahlášení;

2.5.18. sleduje bezpečnostní oznámení dodavatelů svých síťových komponent a patřičně na ně reaguje;

2.5.19. má všechny své weby, na kterých komunikuje se svými zákazníky či obchodními partnery, trvale přesměrovány na protokol HTTPS opatřený TLS certifikátem důvěryhodným v nejrozšířenějších webových prohlížečích, bez tzv. “mixed content” a s vypnutými šiframi, které nejsou považovány za bezpečné.

3. PROVOZNÍ PODMÍNKY PŘIPOJENÍ DO PROJEKTU FENIX

3.1. Člen projektu FENIX

3.1.1. se aktivně účastní pracovních skupin a hlasování v rámci projektu FENIX;

3.1.2. monitoruje komunikaci speciálních e-mailových konferencí (mailing list) určených pro členy projektu FENIX;

3.1.3. je zapojen do systému RTBH filteringu (Remotely-Triggered Black Hole Filtering), kterým se rozumí technika pro zmírnění dopadu DDoS útoků, jejímž prostřednictvím může síť, která je cílem útoku, za pomocí označení určenou BGP komunitou určit, která část provozu se bude blokovat na straně NIX.CZ; pouze z důvodu aktivace systému RTBH a DDoS filteringu může být porušen princip podepisování validních RPKI prefixů podle bodu 3.1.7.;

3.1.4. využívá Route Serverů provozovaných v rámci projektu FENIX, a to zejména k zapojení do systému RTBH a DDoS filteringu popsaných v článku 3.1.3 a k propojení s ostatními členy projektu FENIX;

3.1.5. neužívá připojení prostřednictvím projektu FENIX jako hlavní propojovací platformu pro připojení do uzlu NIX.CZ, pouze v případě, pokud by k tomu byl technický důvod, který člen projektu FENIX oznámí do mailing listu;

3.1.6. využívá pro jeho síť zabezpečení směrování síťového provozu technologii RPKI. Využíváním technologie RPKI se rozumí vytvoření a udržování ROA záznamů vlastněných prefixů. Ve svých vstupních filtrech má nejpozději od 31. ledna 2022 nastaveno odmítnutí nevalidních RPKI prefixů.

3.2. Zapojení do projektu FENIX je realizováno prostřednictvím fyzického portu nebo prostřednictvím 802.1Q.

3.3. BGP relace v rámci projektu FENIX jsou chráněny proti session hijackingu.

3.4. Člen projektu musí zaručit přiměřené aplikování pravidel dle článku 2.5 a článku 3 nejméně v části sítě, jejíž adresní rozsahy propaguje v rámci FENIX VLAN.

4. DOHLED NAD DODRŽOVÁNÍM PRAVIDEL

4.1. Na dodržování Pravidel dohlíží zaměstnanci NIX.CZ, kteří jsou oprávněni průběžně testovat plnění těchto Pravidel (NIX.CZ je oprávněn při takovém testování Pravidla porušit). Zjištěná porušení budou oznamovat členům projektu FENIX. Dotčený člen je oprávněn se k učiněným zjištěním vyjádřit; ostatní členové mohou požadovat vysvětlení či doplnění takových zjištění.

4.2. V případě porušení Pravidel, které zjistí zaměstnanci NIX.CZ podle článku 4.1 nebo člen projektu, včetně případů, kdy člen projektu FENIX přestane splňovat podmínky v článku 3, vyzve ředitel NIX.CZ k odstranění zjištěných nedostatků a stanoví přiměřenou lhůtu. Člen sdružení informuje ředitele NIX.CZ bezodkladně o nápravě nedostatků. Pokud člen nezjedná nápravu, navrhne ředitel NIX.CZ členům projektu jeho vyloučení z projektu FENIX. Opětovný vstup do projektu FENIX je pak možný jen postupem dle článku 2.

4.3. V případě, kdy člen projektu poškozuje svým chováním a komunikací jednotlivé členy nebo projekt FENIX, rozhodnou na návrh dvou nebo více členů Projektu jeho členové o jeho vyloučení.

4.4. Rozhodnutí o vyloučení podle článku 4.2 a 4.3 je přijato, pokud pro něj hlasuje nadpoloviční většina všech členů projektu.

5. ZMĚNY PRAVIDEL A JINÁ ROZHODOVÁNÍ; KOMUNIKACE

5.1. Změnu Pravidel může navrhnout kterýkoliv člen projektu FENIX. Po prodiskutování návrhu vyzve ředitel NIX.CZ členy projektu FENIX k hlasování. Návrh změny je přijat, pokud se pro něj vysloví nadpoloviční většina všech členů projektu FENIX.

5.2. Veškerá komunikace členů projektu FENIX probíhá prostřednictvím zvláštní emailové konference členů projektu FENIX.

5.3. Každý člen projektu FENIX je povinen poskytovat ostatním členům informace o významných bezpečnostních incidentech, k jejichž předcházení či řešení je projekt FENIX určen.

5.4. Hlasování členů projektu FENIX probíhá prostřednictvím elektronického hlasovacího systému zavedeného v NIX.CZ.

5.5. Člen projektu FENIX je povinen zachovávat mlčenlivost o skutečnostech, o kterých se dozvěděl v rámci svého členství v projektu, zejména o veškerých informacích vyměňovaných mezi členy v rámci vzájemné komunikace, o zjištěných bezpečnostních incidentech v sítích jiných členů, o plnění nebo neplnění podmínek dle těchto Pravidel, jakož i o odmítnutí žadatele o členství v projektu FENIX. Tyto informace lze zveřejnit pouze pokud dotčený člen udělil výslovný souhlas se zveřejněním a v případě, že původce informace není znám, souhlas se zveřejněním dali všichni členové projektu FENIX.

5.6. V případě sporu o výkladu některého z ustanovení těchto Pravidel, zejména v případě posouzení, zda došlo k porušení některého z ustanovení těchto Pravidel, rozhoduje ředitel NIX.CZ.

6. PUBLICITA

6.1. Každý člen projektu FENIX má právo užívat zvláštní logo FENIX v provedení schváleném členy projektu FENIX.

6.2. Členové projektu FENIX jsou uvedeni ve zvláštním seznamu členů projektu FENIX umístěném na webu NIX.CZ a vysvětlujícím význam projektu FENIX.